

REMARKS

Claim 1 has been amended. Claims 29-33 have been added. Please charge any claims or other fees for entry of this Amendment to our Deposit Account 03-3415

The Examiner has rejected applicants' claims 1-3 and 4-19 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. In particular, the Examiner states that independent claim 1 recites "a receiving unit that receives one of a first command and a second command, the first command including information indicating one of a plurality of secret keys". The Examiner then states "[n]o where in figures and specification mentions the first command and the second command" and the "[s]pecification has no support of claim limitation, 'the first command including information indicating one of a plurality of secret keys'". This rejection is respectfully traversed.

Applicants submit that the recitations in claim 1 of a "a first command" and "the first command including information indicating one of a plurality of secret keys" is supported by applicants' specification and, in particular, by the description at page 9, lines 5-24 and page 11, line 19, through page 13, line 7. In particular, the "key change command" described in these passages is an example of the recited "a first command". Moreover, the "key number" described in these passage is an example of "information indicating one of a plurality of secret keys". Lines 3 to 5 of page 12 of the specification state that "the key number" . . . is present in the command data field 403 of the key change command".

Additionally, the second command is also supported by the description in applicants' specification at page 15, line 1 through page 16, line 23. Specifically, the signature generation command described in these passages is an example of the second command.

Applicants' specification thus clearly supports the recitation of "a first command (key change command) and a second command (signature generation command), the first command (key change command) including information indicating one of a plurality of secret keys (key number)". Applicants' specification thus describes the claimed invention in such a manner as to permit one of skill in the art to make and use the invention, thereby satisfying the requirements of 35 USC 112, first paragraph. The Examiner's rejection, therefore, should be withdrawn.

The Examiner has rejected applicants' claims 1-3 and 14-19 under 35 USC 103(a) as unpatentable based on the Hirata, et al. reference (JP 2002-300150) taken in view of the Kawakita, et al. reference (JP 10-031326). Applicants have amended independent claim 1, and with respect to this claim, as amended, and its respective dependent claims, the Examiner's rejection is respectfully traversed.

Applicants claim 1 has been amended to better define applicants' invention. Amended claim 1 recites a digital signature generating apparatus that generates a digital signature of digital data, comprising: a receiving unit that receives one of a first command and a second command, the first command including information indicating one of a plurality of secret keys, the plurality of secret keys being included in the digital signature generating apparatus; a secret key changing unit that changes a secret key used by the digital signature generating apparatus to a secret key specified by the first command, if the first command is received by the receiving unit; and a digital signature generating unit that generates the digital signature of the digital data from a hash value extracted from the second command, if the second command is received by the receiving unit. Support for the added underlined feature in amended claim 1 is found on page 15, lines 8-27, of applicants' specification. Newly added claim 29 is a method claim having similar features as amended claim 1.

Such a construction is not taught or suggested by the cited art of record. More particularly, the Hirata et al. reference discloses generating an "electronic signature" by encrypting a "public key PK1 of an IC card 1" with a "publisher's secret key SKI" (paragraph [0007]). Such an electronic signature generating process is not performed in the "IC card 1" but in a "card issuing person device 2". In addition, the electronic signature generating process does not use a hash value of the publisher's secret key SK1 to generate the "electronic signature".

The Hirata et al. reference also discloses that the "IC card 1" generates an "electronic signature S" by encrypting a "public key PK2" newly generated in the "IC card 1" with a "secret key SK1" stored in the "IC card 1" (paragraph [0008]). However, the "IC card 1" neither uses a hash value of the "public key PK2" to generate the "electronic signature S" nor receives the hash value of the "public key PK2" from an external device (such as the "card issuing person device 2").

Applicants note in this regard that the Examiner's statement that the Hirata, et al. reference discloses a "digital signature generating apparatus wherein the digital signal generating unit generates a hash value of the digital data from the digital data in order to generate the digital signature of the digital data" and the further statement that the reference discloses a "digital signature generating apparatus wherein the digital signature generating unit encrypts the hash value of the digital data using the secret key specified by the first command, in order to generate the digital signature of the digital data" are completely unsupported by the teachings of the reference. Nowhere in the passages of the reference cited by the Examiner, i.e., paragraphs 006-008, abstract, claim 1, or elsewhere in the reference, is there any mention or suggestion of using a hash value as in applicant's claims.

The Kawakita, et al. reference was sighted by the Examiner for features unrelated to the generation of an electronic signature. This reference thus fails to adds to the Hirata, et al. reference as to generation of such signatures.

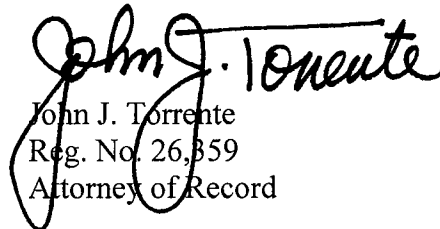
Neither of these references therefore teaches or suggests at least the feature of applicants' amended claim 1 of "a digital signature generating unit that generates the digital signature of the digital data from a hash value extracted from the second command, if the second command is received by the receiving unit." Applicants' amended claim 1, and its respective dependent claims, thus patentably distinguish over the Hirata, et al. and Kawakita, et al. references. Added claim 29, and its respective claims, thus likewise patentably distinguish over these references.

In view of the above, it is submitted that applicants' claims, as amended, patentably distinguish over the cited art of record. Accordingly, reconsideration of the claims is respectfully requested.

Dated: January 21, 2009

Respectfully submitted,

COWAN, LIEBOWITZ & LATMAN, P.C.
1133 Avenue of the Americas
New York, New York 10036
T (212) 790-9200


John J. Torrente
Reg. No. 26,359
Attorney of Record